Pre-print. This is a pre-print of an article published in *Journal of European Integration*. The version of record is available at: https://doi.org/10.1080/07036337.2024.2398434.

Please cite as: Beaumier, G., J. Heering, and A. Newman. 2024. Running out the digital clock: transatlantic privacy politics and veto points in time. *Journal of European Integration* 46 (7): 993–1013. https://doi.org/10.1080/07036337.2024.2398434

Running out the digital clock: transatlantic privacy politics and veto points in time

Guillaume Beaumier[a], Jonas Heering[b] and Abraham Newman[c]

[a]Direction de l'enseignement et de la recherche, École nationale d'administration publique, Québec, Canada
[b]Department of Government, Georgetown University, Washington, DC, USA
[c]School of Foreign Service and Government Departments, Georgetown University, Washington, DC, USA

Corresponding author: Guillaume Beaumier (guillaume.beaumier@enap.ca)

Abstract. Why does the European Commission continue to sign onto unstable international data flow agreements with the United States? After two agreements were struck down by the European Court of Justice, and clear signals that a new one could meet a similar fate, the European Commission agreed to the Data Privacy Framework. To make sense of this behavior, we connect traditional work on veto points with work on historical institutionalism to highlight an international negotiation strategy – running out the clock. While traditional veto points literature suggests multiple institutions with varying preferences will limit the set of potential policies or their adoption, we highlight how these dynamics change when considering veto points in time. We showcase our argument by building three historical narratives detailing the negotiation of the successive data flow agreements. Our findings have important implications for the future of the transatlantic privacy regime as well as negotiation dynamics.

Keywords: Digital economy; data privacy; transatlantic relations; veto points; time

Introduction

> The European Commission [may] be issuing a round-trip to the European Court in Luxembourg – Max Schrems, February 2nd, 2016
>
> The Commission is meant to be the 'guardian of the treaties' and the defender or the 'rule of law' [...] Now the Commission itself simply ignores the Court of Justice for the third time – Max Schrems, July 10, 2023

Since the adoption of the European Data Protection Directive in 1995, the European Union (EU) and the United States (US) have concluded three political agreements (the Safe Harbor Agreement, the Privacy Shield, and the Data Privacy Framework) to allow companies to transfer personal data across both jurisdictions so long as they self-certify their compliance with a set of mutually agreed upon standards. In turn, each agreement plays a crucial role in sustaining the transatlantic digital economy at the heart of this special issue (Young 2024a). Behind the veneer of cooperation, though, the successive negotiations highlight the challenges that the US and the EU face in governing the transatlantic digital economy.

Following the decision by the European Court of Justice (ECJ) in 2015 to strike down the Safe Harbor Agreement for failing to provide an adequate level of protection against American

surveillance practices, the transatlantic partners have struggled to create a lasting legal solution. As highlighted in the first quote in the epigraph of this article, minutes after Privacy Shield, the second data flow agreement, was adopted, Max Schrems, the activist behind the complaint that led to the Safe Harbor's demise, announced his intent to challenge it in courts. Four years later, the ECJ sided with him and invalidated the Privacy Shield.

Despite the agreement on a new Data Privacy Framework, its long-term fate remains uncertain. Schrems, now chairman of the non-governmental organization, *none of your business* (noyb), was quick to denounce the new framework for not addressing the concerns raised by the ECJ, as highlighted in the second quote in the epigraph, and vowed to challenge it again. Meanwhile, Didier Reynders, European Justice Commissioner, expressed uncertainty as to whether the new deal would survive, saying it had a '7 or 8 chance out of 10' to be upheld in court (Manancourt 2022). The European Data Protection Board, which advises the European Commission on international adequacy decisions, voiced concerns as the new privacy agreement's 'principles remain essentially the same as under the Privacy Shield'.

This pattern of repeated European compromise is quite surprising given standard literature on EU regulatory power as well as existing research on the role of veto points in international negotiations. In recent years, scholars promoted concepts like 'market power' (Damro 2012; Drezner 2007) or 'normative power' (Kelemen 2010; Manners 2002) to describe the European Union's capacity to project its rules globally. Following similar insights, Anu Bradford coined the term 'Brussels effect' to describe what she saw as the growing tendency of European regulators setting global rules (2012). Bradford highlighted the tendency for companies outside of Europe to adopt more stringent European rules to gain access to its lucrative market. Data privacy offered a prime example of this phenomenon whereby American firms should prefer to abide by European regulations, allowing them to simultaneously operate in the US and the EU (Bradford 2012, 22–25). In keeping with standard accounts of veto points, the ECJ's authority to enforce European rules independently should reinforce this effect by credibly tying the Commission's hand in a kind of two-level game (Putnam 1988). Nevertheless, the Commission proceeded to negotiate three agreements with the United States, each facing significant domestic opposition.

Rather than an extension of EU power or a case of tying of hands, we argue the successive data privacy deals offer a window into a less understood negotiating strategy – running out the clock. Here, we connect work on veto points to work on historical institutionalism and explore what happens as executives consider veto point politics as embedded in time. Our key observations is that the activation of veto points is not always immediate. Courts, legislatures, or referenda can often take years to organize, review and decide on international agreements. Given the potential for such delays, executives may seek to advance their agenda, making temporary gains, while hoping for a change in the preferences of key veto player or for a broader change in the policy conditions that might resolve the conflict in their favor.

In the case of transatlantic data privacy dispute, the European Commission had considerable economic incentives for maintaining cross-border data flows but faced repeated signals that it would face judicial review, leaving the Commission in a tenuous political position. The political agreements temporarily resolved the threat of economic disruption, while playing on the uncertainty of the stability of the European Court of Justice's preferences over time. During

the gap between the negotiation of each agreement and their review by the ECJ, the court's interpretation of EU law could evolve, the United States could adopt a comprehensive federal data privacy law, or other changes could alter the nature of the regulatory conflict. In the meantime, the Commission gained by supporting the growth of the transatlantic digital economy (Young 2024a). As noyb (2023) has complained, despite the ECJ nullifying two transatlantic data flow agreements, businesses have been able to continue transferring personal data across the two jurisdictions for over two decades.

In addition to mapping the trajectory of transatlantic data privacy negotiations over the last quarter century, we bring a temporal perspective to the study of veto points. International relations and comparative scholars (Mansfield, Milner, and Pevehouse 2007; Tsebelis 2002) often study how the constellation of domestic veto points at a specific point in time can affect policy decisions. We highlight how actors may sign onto agreements that run counter to current domestic veto point constellations given the uncertainties associated with the stability of such constellations. This helps explain why executives may sign onto international agreements that seem doomed to domestic political failure at the time of their signature. Equally important, our article helps shed light on what appears to be the chaotic nature of EU cooperation on data privacy in the transatlantic space, helping policymakers anticipate future crisis.

Running out the clock: navigating judicial veto points in time

The study of veto points has a long tradition in comparative politics (Hallerberg and Basinger 1998; Tsebelis 2002) and international relations (Mansfield, Milner, and Pevehouse 2007; O'reilly 2005). At its core, it argues that polities with more veto points support the status quo. Veto points refer to institutional actors with the ability to block policy change and can notably be legislative, partisan, or judicial actors. As the number of veto points grows and more actors need to give their consent for a policy change, the likelihood of the latter being blocked increases. George Tsebelis (1999, 2000, 2002) is generally credited for specifying that more than just their number, the ideological distance between actors controlling veto points, or veto players, will determine the size of the 'winset' for policy change, or the number of solutions that can alter the status quo. In effect, if all veto players shared the same ideological position, their number would not matter since they would all defend the same position.

Evidence supporting the veto points argument is now widespread. Scholars have shown how the presence of multiple veto points with different preferences affected changes in taxation policies in OECD countries (Hallerberg and Basinger 1998), welfare policies across European countries (Bonoli 2001; Obinger, Leibfried, and Castles 2005), and the adoption of comprehensive data privacy laws in the United States and Europe (Newman 2008). Conversely, some argued veto points increase the credibility of policy commitments (Keefer and Stasavage 2003; Mansfield, Milner, and Pevehouse 2007). They demonstrate that as veto points make policy change more difficult, they send a signal of stability to domestic and foreign audiences. Once a new policy is adopted, veto points will limit departure from this new status quo, just as they constrained its adoption in the first place.

At the international level, domestic veto points can similarly alter the size of the winset of negotiated outcomes. Following work on the two-level game (Putnam 1988; see also Young

2024b this issue), the presence of multiple and ideologically distant veto points constrains that country's executives in negotiations, reinforcing the status quo. Looking at trade negotiations, Mansfield, Milner, and Pevehouse (2007) find that countries with more domestic veto points are less likely to conclude preferential trade agreements. Figure 1 represents this argument graphically in a simplified unidimensional space. Country A has one institution with veto power (A_1) and country B two (B_1 and B_2). Each bracket showcases the most distant policy that would fit an institution's preference, starting from their respective countries' negotiation position. While the policy preferences of A_1 and B_1 showcase a positive winset, with X representing a mutually acceptable agreement, there are none possible when considering the policy preferences of B_2. Following the traditional veto point argument, the constellation of preferences shown in Figure 1 should lead to a breakdown of the negotiation.

The question then remains as to why an executive might sign onto an agreement, in the face of a domestic veto point. One potential explanation from the two-level game literature is misperception. In most cases, executives operate under incomplete information about their domestic veto points' preferences (Evans, Jacobson, and Putnam 1993, 411–412; Milner and Rosendorff 1997). While misperception can sometimes lead to an early breakdown in the negotiation by exaggerating the perceived distance between domestic veto points (see Brown 2024 this issue), it can also do the contrary. Executives may agree to deals they believe fulfill their domestic veto points to see them later being vetoed. The temporary veto of the trade agreement between Canada and the EU by the government of Wallonia represents an instance where European and Canadian negotiators failed to anticipate Wallonia's opposition and, to some extent, its veto power due to the particular EU integration structure (Bursens and De Bièvre 2023).

Following this misperception argument, we should expect that when a domestic institution uses its veto power, it also provides more information about where it stands and what type of policies would gain its support. In addition to making the threat of a future veto more credible, it simultaneously removes some uncertainty about the constellation of domestic veto points' preferences. Concomitantly, it should prevent executives from signing new agreements that would not fulfill the preferences of one of its domestic institutions with veto power. Looking again at Figure 1, if B_2 vetoed agreement X, we should not expect the executives from country B to agree on agreement Y even though it is now closer to B_2 's expressed preferences. A situation where executives would successively misread the preferences of their domestic institutions and sign soon-to-be vetoed agreements seems especially unlikely.

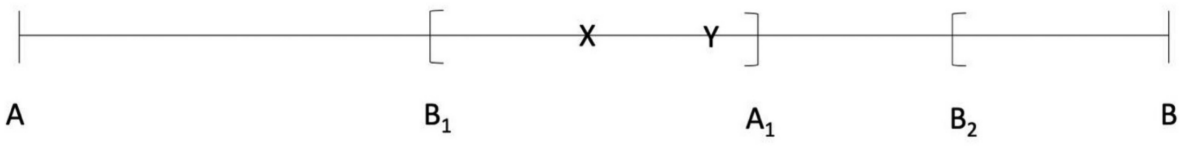


Figure 1. Winset with veto points (inspired from Putnam 1988).

In this article, we build an alternative explanation for why executives may sign onto an international agreement in the face of domestic opposition by more explicitly situating veto point politics in time. When building his original theory of veto players, Tsebelis (2002, 33–34)

suggested that the sequence in which political actors controlling veto points act will influence final policy outcomes. Those acting first can chiefly take other veto players' preferences as constraints in determining their preferred course of actions. As they consider the set of potential policies that would fulfill their and others' policy preferences, they can choose the closest one to their ideal policy solution. Tsebelis calls this the 'agenda-setting advantage' (2002, 34).

We build on this insight to argue that agenda-setter's policy choices may depend in part on the uncertainty surrounding the persistence of veto players' preferences as they move into the future. The use of veto points rarely happens immediately. There is often a lag between the negotiation phase of an agreement and the implementation or review of the agreement in the domestic political systems. During that period, the nature of the veto point constellation may change. Milner and Rosendorff (1997), for example, note that by creating uncertainty and raising the risks of ratification failures, upcoming legislative elections may incentivize the executive branch to negotiate international agreements under existing favorable conditions. Alternatively, an executive facing opposition could gamble on domestic veto points moving closer to their preferences over the timeframe between agreement and veto point activation. Figure 2 presents this graphically. The dotted bracket represents the most distant policy B_2 could accept in the future. An executive B_1 from country B may play on the temporal uncertainty around domestic institution B_2 's preferences and negotiate agreement X, which appears impossible in the current period but possible if B_2 moves to $B_{2'}$.

This temporal effect is present in a host of EU negotiating dynamics as the implementation phase of international agreements is often drawn out through national parliamentary approvals or judicial review. The temporal dynamic is particularly important for judicial veto points as they can take years before exercising their veto power. For simplicity, Tsebelis explicitly put judicial veto points aside when building his theoretical argument (Tsebelis 2000, 447). Courts are however important veto points and judges are political actors with their own policy preferences, which affect how they interpret legal obligations (Voeten 2008). In the EU, the ECJ is often referred to as an 'activist court', notably for its role in promoting European integration (Terpan and Saurugger 2019). Others have emphasized how the ECJ also acts as a policy leader by adopting innovative interpretations of EU law forcing, in some instances, the Commission to alter its policies to protect the EU's fundamental values (Mandujano Manriquez and Pavone 2024).

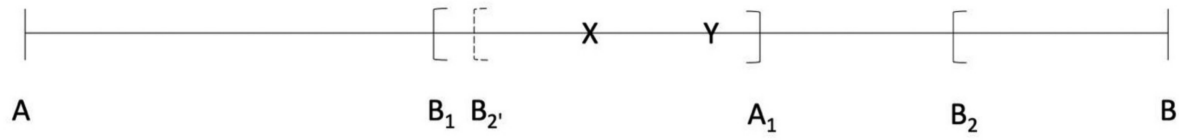


Figure 2. Winset with veto points in time.

The temporality of judicial veto points creates an opportunity for executive bodies acting as agenda-setters to push for policies closer to their preferred outcome. Knowing it might be years before their policy gets overruled, they may bet on circumstances changing to their advantage. The political environment can change, judges can turnover, or case-law can evolve, creating more favorable conditions for their preferred policy.

Moreover, while the application of judicial veto points is delayed, there can be short-term benefits from reaching a deal. Faced with pressing socio-economic issues, executive actors may want to sign international agreements challenging the status quo. As years may pass before a judicial actor vetoes the agreement, the executive can gain from temporarily resolving a difficult cooperation problem, which may even get resolved before the policy is finally, if ever, reviewed by courts. The adoption of the agreement may also present a fait accompli, which shapes the positions of industry and civil society vis-à-vis the issue. By 'running out the clock', an executive may sign onto an agreement which appears destined for failure in the current veto point constellation, playing on the uncertainty associated with that constellation by the time the veto player will be able to exercise its authority. In the worst-case scenario, this strategy can buy time while the executive looks for other solutions to achieve their preferred outcome. In the best-case scenario, the executive reaches its preferred solution more quickly than otherwise possible.

In contrast to the traditional misperception argument in two-level game theory, the argument is not that executive actors fail to grasp the preferences of judicial veto points and unknowingly sign agreements doomed to fail. Rather, executive actors know they can make temporary gains by signing an arrangement resolving a cooperation problem while new circumstances may change the court's position before it is able to act.

Our theory is agnostic to the specific motivations that drive executives to adopt the 'running out the clock strategy.' In other words, it does not require executive actors to act in bad faith. Well-intentioned actors may attempt to sign an agreement closer to the courts' preferences, such as agreement Y in Figure 2, thereby decreasing the likelihood of a future veto. At the same time, executives may also intentionally sign onto agreements they know violate domestic laws if they have strong (geo-)political or economic incentives to engage in such strategic non-enforcement. Here, buying time allows executives to, at least temporarily, circumvent costly regulations, similar to how private companies have used lengthy court proceedings to stall regulatory enforcement and continue reaping profits (Mazur and Serafin 2023). Others have highlighted how policy non-enforcement can be linked to states industrial policy strategies, for example (Dewey and Di Carlo 2022).

Regardless of their intentions, executives acting as agenda-setters with delayed judicial veto points do not have infinite discretion. There can be significant costs associated with a court's vetoing of a policy, even years after its adoption. Governments pushing for policies found unconstitutional can lose legitimacy, impacting their chance of staying in power. Blatant violations can also attract public outcry, and, in some cases, courts may quickly exert their veto through injunction measures. As such, it is essential that policies remain on their face legally valid – or that there is sufficient uncertainty regarding their legal validity – for this strategy to be effective. In cases where a court has vetoed a previous agreement, it is important that executive actors can at least demonstrate an attempt to answer the concerns raised in the judicial decision and get closer to the courts' expressed preference. An executive actor may nevertheless be aware that a new agreement remains at risk of being vetoed.

Table 1 summarizes the three explanations discussed and their respective expectations. We hereafter contextualize the transatlantic dispute over data flows and privacy before showcasing

Table 1. Three explanations and expectations based on veto points.

	Traditional veto points	*Two-level game theory*	*Running out the clock*
Preferences	Fixed	Fixed	Changing
Uncertainty	No	Yes	Yes
Logic	Breakdown	Miscalculation	Buying time
Expectation	No agreement is reached	One agreement gets vetoed in court, clarifying the courts' preferences and impeding future agreements	Multiple agreements test the boundaries of courts' preferences, while providing temporary gains

how the argument based on judicial vet points in time help explain the successive negotiation of three international data flows agreements between the EU and the US.

The transatlantic privacy dispute

The transatlantic dispute over cross-border data flows reflects ongoing differences in the US and EU's approaches to privacy regulation. Despite each jurisdiction broadly agreeing on the need to ensure individual control over the collection and use of their personal information, they significantly differ over *how* to achieve this goal, or in the politics rather than the principles of privacy (see Young 2024a this issue). In effect, while both broadly embrace a liberal view of privacy (Bennett and Raab 2006), they fundamentally differ in their regulatory approach with significant consequences for transatlantic data flows. While often associated with Europe, data privacy emerged as a governance regime from interactions across the Atlantic, culminating in the adoption Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (Beaumier, Papin, and Morin 2024, 64). Over the years, various studies have shown that both jurisdictions tended to converge around similar norms (see e.g. Bennett 2010; Gunst and De Ville 2021). Yet, their lasting disagreement is over the scope and enforcement of privacy rules (Newman 2008).

In the EU, the 1995 Data Protection Directive (DPD) established common rules with regards to the collection and use of personal data by private companies. Importantly, the DPD also gave European regulators clear authority over access to its single market for information (Bach and Newman 2007, 835). Under Article 25, personal data collected in Europe could only move transnationally if the destination jurisdiction demonstrated that it had an 'adequate' level of privacy protections. It was left to the Commission, in collaboration with a newly created transgovernmental group comprised of representatives from each EU member state data protection authorities, the Article 29 Working Party, to determine whether another country's privacy protections were adequate. If not, its companies would face the choice to either stop using European data or establish a physical presence in Europe and separate their activities at potentially significant costs.

In 2018, the EU strengthened its comprehensive privacy regulation through the introduction of the General Data Protection Regulation (GDPR). In addition to establishing new substantive obligations, such as the so-called right to be forgotten, and becoming directly enforceable in EU Member States, the GDPR expanded the scope of EU privacy protections. It covers new types of personal data, including IP addresses, but also companies without a physical establishment in

the EU offering goods or services to people located in the EU (Kalyanpur and Newman 2019). Moreover, it establishes a new formal body, the European Data Protection Board (EDPB), to replace the Article 29 Working Party to oversee the implementation of the GDPR across EU Member States and coordinate implementation amongst national data protection authorities (Li and Newman 2022).

Just as the EU emphasized the importance of public oversight, the US has prioritized industry self-regulation (Schwartz and Pfeifer 2017, 146). The White House's first official policy document on e-commerce directly encouraged firms to set up a voluntary self-regulatory framework (Farrell 2003). Rather than a comprehensive privacy law, the US privacy regime nowadays consists of a range of sectoral laws, covering certain types of health data and children's privacy, industry self-regulation, and, most recently, some more comprehensive laws at the state level (Beaumier 2023; Chander, Kaminski, and McGeveran 2021). Importantly, the US federal government lacks an independent agency dedicated to data privacy issues.

In the absence of an effective multilateral regime governing transnational data flows (cf. Shahin 2024 this issue), the two sides' divergent approaches to privacy regulation, coupled with the extraterritorial reach of EU privacy rules, became the source of repeated conflicts. The lack of a privacy law covering the private sector at the federal level chiefly impedes the US from being straightforwardly considered as offering an adequate level of privacy protection, with potentially devastating costs for the transatlantic digital economy. In addition to limiting the export of increasingly valuable digital services, any disruption to transatlantic data flows could pose challenges for the development of artificial intelligence and complicate cybersecurity cooperation (Birchfield 2024; Fahey 2024 in this issue).

In this context, the European Commission and the US government have remained keen on finding a negotiated solution. Since the Snowden revelations highlighted the scope and extent of American surveillance practices, the ECJ has positioned itself as the guardian of European privacy standards, striking down two agreements for failing to provide an adequate level of protection. In the following section, we present how the Commission attempted to navigate the ECJ veto point by running out the clock following the demise of the original Safe Harbor agreement. Despite repeated and unambiguous warnings from actors inside and outside the EU that each new deal was unlikely to survive legal contestation, we show how the Commission attempted to assuage the ECJ's concerns and temporarily resolve the conflict while hoping new circumstances offer a more durable solution.

Negotiating transatlantic data flows agreements

The Safe Harbor agreement

The negotiation of an EU-US data flow agreement first became a policy priority in the wake of the adoption of the DPD. As it became clear that American companies could not benefit from exceptions provided in the DPD (Farrell 2003; Long and Quek 2002), American and European authorities started to negotiate on the possibility for the US to be officially considered as offering an adequate level of protection.

At the time, the lack of comprehensive privacy legislation and especially the absence of official recourse available to EU individuals to challenge the use of their information by American

firms impeded the US from meeting an adequate level of protection (Long and Quek 2002, 334). A breakthrough in the negotiation came from the introduction of the concept of a 'safe harbor' by American negotiators (Farrell 2003). Inspired by similar mechanisms in American law, they suggested setting up a voluntary certification regime to which individual US firms could sign up and, in doing so, be considered as providing an adequate level of protection. After nearly two years of negotiation, the Commission agreed to this idea, signed onto the Safe Harbor agreement, and adopted an adequacy decision based on the latter, on 26 July 2000.

In practice, it represented a *partial* adequacy decision, whereby only a limited subset of firms were allowed to transfer personal data from the EU to the US. Firms that joined Safe Harbor had to agree to a set of privacy principles, including allowing individuals to opt out of having their data used for certain purposes or having their data transferred to a third party. The enforcement mechanism for Safe Harbor consisted of a hybrid structure that combined the US-preferred approach of self-regulation with the EU's demand for government oversight: self-regulatory bodies provided participatory firms with a seal that signaled their compliance with the Safe Harbor principles, the US Federal Trade Commission (FTC) monitored the self-regulation scheme and could fine non-compliant firms, and the Commission retained the authority to withdraw its adequacy decision at any time.

For the Commission, the Safe Harbor agreement offered a way to keep data flowing across the Atlantic while simultaneously working to protect Europeans' privacy. Despite some opposition at first, all EU Member States approved the agreement (Farrell 2003, 294). There was also little indication at the time that the agreement would be struck down by the ECJ. While representatives from the European Parliament initially threatened to challenge the Safe Harbor agreement before the ECJ, due to concerns that the agreement provided inadequate protections for Europeans' privacy, Commission officials successfully convinced them it was the best possible outcome (MacMillan 2000). EU officials even seemed optimistic that Safe Harbor could serve as a model to resolve regulatory conflicts in other issue areas (Farrell 2003). Moreover, the adequacy standard required under the DPD remained relatively vague. Article 25 did not define 'adequate' and only specified that it should be assessed 'in the light of all the circumstances', leaving considerable room for interpretation (Litan and Swire 1998, 32).

For more than a decade, Safe Harbor successfully facilitated transatlantic personal data flows. While European privacy activists and officials lamented the lack of clarity and enforcement of the agreement (Farrell and Newman 2019), the Commission reaffirmed its support of Safe Harbor in a joint statement with the American government (US Department of Commerce 2012). By that year, the value of EU-US trade in digital services, which relied on frictionless transatlantic data flows, had grown to nearly $227 billion, a significant portion of the approximately $1 trillion overall EU-US trade in goods and services (Meltzer 2016, 1).

But Safe Harbor began to unravel in 2013, when former NSA contractor Edward Snowden revealed the vast scope of US government surveillance, including data collected by US companies participating in the Safe Harbor agreement. The Snowden leaks highlighted the contradictory legal obligations that American internet companies faced under Safe Harbor and US surveillance laws, and it became clear that companies frequently violated the principles of the former to comply with the latter. In response to the leaks, the Commission announced that it would review

Safe Harbor (Farrell and Newman 2019).

The exposure of the link between commercial data flows and government surveillance also allowed European privacy activists to challenge Safe Harbor. Shortly after the Snowden leaks were published, Max Schrems, an Austrian privacy activist, filed a complaint with the Irish Data Protection Commission against Facebook, alleging that the company's data transfers to the US violated Safe Harbor because they exposed Europeans' personal data to surveillance by US authorities (Farrell and Newman 2019). The case, which became known as *Schrems I*, was eventually referred to the ECJ, which declared the Commission's Safe Harbor adequacy ruling invalid in October 2015. The court wrote that US surveillance practices 'disregard, without limitation, the protective rules laid down by [Safe Harbor]' and that the 'scheme thus enables interference, by United States public authorities, with the fundamental rights of persons' (European Court of Justice 2015, 2).

The *Schrems I* decision reshaped transatlantic data flow politics in two significant ways. First, the ECJ decision emphasized the court's authority to declare the Commission's adequacy decisions invalid and reinforced the position of national privacy authorities vis-à-vis the Commission in the regulation of trans-border data flows. In so doing, it elevated the importance of both the court and the national data protection authorities as veto points for future transatlantic data flow agreements. Second, in its decision, the ECJ also clarified the meaning of the adequacy standard, noting it should be 'essentially equivalent' to the European level of privacy protection (European Court of Justice 2015, 2). As such, it effectively raised the threshold any future agreement would have to reach to fulfill its veto point.

The failure of the original Safe Harbor agreement is consistent with standard miscalculation accounts at two levels. At the international negotiation level, the Snowden revelations first made clear that data flow agreements were not immune to extensive American surveillance practices. Shortly after the leaks, the European Commissioner in charge of privacy matters, Viviane Reding, declared the 'Safe Harbour agreement may not be so safe after all' (European Commission 2013). Reading subsequently insisted on legislative changes in the US to ensure the protection of EU citizens' right to privacy (O'Donnell 2013).

At the domestic level, the Commission learned new information regarding the position of the ECJ. Prior to the Snowden revelations, the Commission had credible reasons to believe that Safe Harbor provided 'adequate' protections for EU individuals' data. The *Schrems I* decision removed much of this uncertainty by clarifying the meaning of an adequate level of protection and pointing to conflicting obligations under US domestic law as a key reason that Safe Harbor failed to meet this adequacy standard. Moreover, by exposing the limitations of the EU's data privacy rules in protecting cross-border data flows, *Schrems I* also helped push forward the implementation of the GDPR (Laurer and Seidl 2021). Considering the new information available to the Commission, and the imminent strengthening of the EU's internal rules, a new agreement appeared unlikely in the absence of legislative change in the US or other new circumstances that could otherwise change the ECJ's position. Nevertheless, the Commission quickly started to negotiate a new agreement with the US, reflecting a strategy to buy time.

Privacy shield

While the Snowden revelations made clear that privacy protections offered in the Safe Harbor framework could not muster the adequacy test, economic realities provided strong incentives for the EU to secure a new agreement. When releasing its Digital Single Market strategy in 2015, the European Commission (2015) emphasized the EU's heavy dependence on the US, with more than half of online services being provided by American firms. Moreover, transatlantic data flows had grown rather one-sided: by 2012, the EU imported nearly 63% more in digitally-enabled services from the US than it exported (Meltzer 2016, 1).

In early February 2016, only four months following the ECJ decision, EU and US negotiators announced they had reached a political agreement to replace Safe Harbor with a new framework called Privacy Shield. Privacy Shield included several improvements over Safe Harbor, including a strengthened monitoring and enforcement regime, annual joint EU-US reviews of the framework, and the appointment of an Ombudsperson that would handle EU citizen's complaints and inquiries regarding the abuse of their data by US intelligence agencies. Yet, besides the Commission's adequacy decision, Privacy Shield still relied on non-binding commitments from the US side (Fahey and Terpan 2023).

Despite these proposed changes, several actors on the EU side immediately raised concerns about the viability of this new agreement. Before the Commission issued its adequacy decision, the Article 29 Working Party (2016) issued an opinion in which it criticized the proposed redress mechanism, notably questioning the independence of the ombudsperson. The European Parliament (2016) issued a resolution calling on the Commission to reopen the negotiations over Privacy Shield to address the agreements' deficiencies pointed out by the Working Party. Meanwhile, in an exchange of letters to then-Justice Commissioner Věra Jourová, the European Ombudsperson (2016a, 2016b) criticized the proposed Ombudsperson mechanism for its lack of independence and, most likely, failing to fulfill the standard set by the ECJ.

As the first quote in the epigraph to this article indicates, Max Schrems (2016), the privacy activist behind the invalidation of the Safe Harbor, made clear he would again challenge the agreement in courts, threatening to activate the Court's veto point even before the adoption of the agreement. Considering that the ECJ's *Schrems I* decision sent a clear signal that the Court would act as a veto point for future agreements that failed to provide 'essentially equivalent' protections for EU individuals' data abroad, combined with the lack of any fundamental change in privacy law in the US, Privacy Shield seemed bound to follow the unfortunate fate of its predecessor. Nevertheless, the Commission issued an adequacy decision and Privacy Shield went into effect (European Commission 2016).

Discussing the agreement prior to the first joint annual review, Giovanni Buttarelli, European Data Protection Supervisor and highest privacy official in the EU, argued that the deal could only be 'an interim instrument for the short term' and that 'something more robust [needed] to be conceived' (Stupp 2017). He added the EU should follow a two-track approach, aiming to ensure the conditions of the deal are satisfied in the short term and work to create broader change in US law in the long term (Stupp 2017). By securing another data transfer deal with the US, the Commission was able to avoid a potentially costly outcome. While working on building its digital single market, European negotiators could also work with their American

counterparts to promote greater convergence in privacy protection. In the worst-case scenario, the ECJ's judicial veto point would take years before striking down the deal and the EU would have had time to hopefully reduce its dependency on US firms. In a best-case scenario, the US would adopt new measures making the Privacy Shield agreement unnecessary in the future.

In the end, the ECJ struck down the Privacy Shield in July 2020 in what became known as *Schrems II*. Echoing the concerns that had been raised by privacy activists and European officials since the inception of the agreement, the court argued US surveillance practices of transatlantic data flows remained in violation of EU law, including under the EU's updated privacy regime, GDPR, and that EU citizens still had no effective redress mechanisms to excessive surveillance under US law. This ruling left transatlantic data flows again in a legal limbo.

Whereas the decision to agree to Safe Harbor may be attributed to miscalculation regarding the likelihood of the ECJ to veto the agreement, the *Schrems I* decision clarified the position of the ECJ as a veto player. Yet, Privacy Shield, while including many improvements over Safe Harbor, still largely relied on non-binding commitments by the US. Buttarelli's comments reflected an understanding on the EU side that Privacy Shield would only provide a temporary solution and the hope that an agreement would give time for additional changes to happen in US law.

EU – US data privacy framework

Following the *Schrems II decision*, the Commission was reluctant to renegotiate another transatlantic data flow agreement. Economic incentives were still strong as nearly 5,400 businesses had come to rely on Privacy Shield, contributing to $264 billion in ICT-enabled trade between the EU and the US in 2020 (Fefer and Archick 2021, 1). Halting transatlantic data flows altogether was estimated to result in a loss of 330–420€ billion of EU GDP (5). At the same time, *Schrems II* made it clear that the Court believed that the US lacked an adequate level of protection in the absence of a comprehensive federal privacy law, or at the very least an independent regulator with the power to review US agencies' surveillance practices. Efforts by US lawmakers to pass any such legislation had remained stagnant (Kerry and Chin-Rothmann 2020).

Nevertheless, the Biden administration made securing a new agreement on transatlantic data flows a political priority. American negotiators offered to upgrade the ombudsperson system to a panel of independent judges that would review European challenges to data collection practices by US national security agencies (Scott 2021). In line with the ECJ's latest decision, the EU initially resisted these proposals and demanded legislative changes to US surveillance laws, not just a presidential executive order, as a precondition for a new agreement. In a speech in June 2021, EC Vice President Věra Jourová emphasized that 'A legally-binding rule would be very useful, I would even say necessary' (Scott and Manancourt 2021). EU officials also opposed the Biden administrations' attempt to fold discussions over a data sharing agreement into the newly created EU-US Trade and Technology Council (Manancourt and Scott 2021).

While negotiations stalled, the full economic repercussions were on hold as transatlantic data flows continued in practice using Standard Contractual Clauses (SCCs). Individual firms pledged to uphold privacy principles through legal contracts. However, observers noted the viability of data transfers through SSCs was questionable (Manancourt and Scott 2021). These concerns

were finally confirmed when, in May 2023, the Irish Data Protection Commission fined Meta a record fine of 1.2 billion Euro for violating the GDPR because the company had continued to transfer Europeans' data to the US using SSCs without taking sufficient safeguards (European Data Protection Board 2023a). Following the Irish data protection authority's decision, Meta faced a suspension of transatlantic data flows relying on SSCs by October 2023. Meanwhile, transatlantic data flows by American platforms had become an integral part of EU member states response to COVID-19, as some government's contact tracing apps relied on technical infrastructure provided by US firms. Uncertainty surrounding the viability of SSCs, and the October deadline, put greater pressure on the Commission to negotiate a new agreement.

The need to replace Privacy Shield gained additional urgency for the Commission in the wake of Russia's invasion of Ukraine. Both American government officials and representatives of Big Tech firms stressed the importance of unimpeded transatlantic data flows to allow US intelligence agencies to provide intelligence to European partners and for US firms to contribute to protect Ukraine from cyberattacks (Scott and Manancourt 2022). Commission officials noted that the war, and the importance of data flows to cyber defense efforts, had elevated the importance of democracies to work together, calling even for a global data privacy agreement (Stupp 2023). A month after the invasion, President Biden and Ursula von der Leyen, President of the European Commission, announced that they had reached an agreement in principle on a Transatlantic Data Privacy Framework (DPF) (The White House 2022). In a statement posted on X (formerly Twitter), Von Der Leyen (2022) presented the DPF as 'another step in strengthening [the transatlantic] partnership,' thereby directly linking the data flow agreement to broader geopolitical concerns.

The DPF retains the self-certification scheme at the core of both Safe Harbor and Privacy Shield but includes 'binding safeguards to limit access to data by US intelligence authorities to what is necessary and proportionate' as well as an improved redress system that includes the creation of a Data Protection Review Court (European Commission 2022). Significantly, only citizens from 'qualifying jurisdictions,' i.e. countries offering sufficient privacy safeguards to American citizens' data, allowing data transfers to the US, and supporting US national interests, will have access to this new mechanism. The US Department of Justice made this qualification, creating a form of reciprocity in the adequacy decision process (Propp 2023). These improvements are meant to address the specific issues that the ECJ raised again in *Schrems II*. Legal scholars emphasized the DPF represents a movement toward a hardened legal framework (Fahey and Terpan 2023). As such, some are positive that the new agreement could prove enough to fulfill the Court's equivalency standard (Christakis, Propp, and Swire 2022; Kerry 2023).

However, the DPF and the prospective adequacy decision are still based on an Executive Order by the Biden administration, rather than legislative changes in US surveillance laws as EU officials originally requested. Shortly after the details of the proposed agreement became public, several EU institutions that had already voiced concerns over Privacy Shield reiterated their skepticism toward the DPF. In February 2023, the EDPB issued an opinion on the Commission's draft adequacy decision, in which it noted that DPF offers 'substantial improvements' to the proportionality of US surveillance activities and the redress mechanism for Europeans'

complaints, but it also argued that 'the DPF Principles [...] remain essentially unchanged with regard to those applicable under the Privacy Shield' (European Data Protection Board 2023b). The European Parliament was even more direct in its criticism of the new framework. In April 2023, the EP's Civil Liberties Committee (LIBE) issued a resolution on the DPF in which it urged the Commission not to issue an adequacy decision because the committee was 'not convinced that this new framework sufficiently protects personal data of our citizens, and therefore we doubt it will survive the test of the CJEU' (European Parliament 2023). In particular, LIBE noted that the DPF did not provide sufficient protections from US intelligence agencies' bulk collection of personal data, which was a key concern that the Court had raised in *Schrems II*. Even the EU's Justice Commissioner, Didier Reynders publicly stated that he gives the DPF a 'seven or eight out of 10 chance' of withstanding another legal challenge by the ECJ – hardly a resounding vote of confidence (Manancourt 2022). Meanwhile, Schrems criticized the deal for being 'structural insufficient' and merely 'buying another couple of years' (Noyb 2022).

Despite receiving clear signals that the DPF would again fall under the scrutiny of the Court, the Commission issued an adequacy decision for the DPF on 10 July 2023 (European Commission 2023). Unsurprisingly, Schrems, and his organization, noyb, were quick to denounce the new framework. Schrems stated that:

> We now had 'Harbors', 'Umbrellas', 'Shields' and 'Frameworks' - but no substantial change in US surveillance law. The press statements of today are almost a literal copy of the ones from the past 23 years. Just announcing that something is 'new', 'robust' or 'effective' does not cut it before the Court of Justice. We would need changes in US surveillance law to make this work - and we simply don't have it. (Noyb 2023)

He also reiterated the DPF is little more than an attempt by the Commission to buy time: 'Just like "Privacy Shield" the latest deal is not based on material changes, but by political interests. Once again the current Commission seems to think that the mess will be the next Commission's problem' (Noyb 2023). Other stakeholders shared Schrems' assessment of the Commission's strategy. Moritz Körner, a Member of the European Parliament from the German liberal party, called the agreement 'old wine in new bottles' (Beutelsbacher 2023). Meanwhile, a former German data protection commissioner, Thilo Weichert described the DPF as a 'labeling scam' and merely a 'temporary solution' for transatlantic data flows (Beutelsbacher 2023).

For the Commission, a deal that buys at least a few more years offers considerable benefits. For one, it helps maintaining transatlantic unity in the context of growing geopolitical tensions. Faced with the war in Ukraine and China's rise, there is a need for European leaders to present a united front with their American counterparts. Following the *Schrems II* decision, Wojciech Wiewiórowski, the European Data Protection Supervisor, noted that the US and EU are 'much closer' than often assumed while adding he preferred 'data being processed by entities sharing European values' (cited in Swire 2020). Moreover, the new agreement ensures American platforms can continue to operate in Europe following the ban of SCCs as an alternative method of data transfer. In the end, the new framework agreement entered into force a few months before Meta, and most likely other American companies soon after, faced a suspension of data flows (Humphries 2023). The twin concerns of war and economic disruption proved an important impetus for even short-term action.

At the same time, observers noted that the prospect of changes to US privacy law might in the interim change the Court's calculus. Several legislative proposals had surfaced for federal privacy legislation, such as the American Data Privacy and Protection Act (ADPPA), which could provide legal certainty for transatlantic data flows (Fahey and Terpan 2023). Despite the ADPPA never making it to a vote in the US House of Representatives, federal privacy legislation has received some new political interest amid US lawmakers' demands for protections for minors and concerns about surveillance by the Chinese-owned social media platform TikTok (Holland 2023).

Even without legislative change, the evolving norms surrounding acceptable surveillance practices may come to support a positive assessment of the DPF by the ECJ. In *Schrems II*, the court refused to grant any 'margin of discretion' to the US government in balancing surveillance activities and privacy guarantees in democratic societies, sidestepping in the process jurisprudence from the European Court of Human Rights (Kerry 2023; Propp 2023). A renewed challenge could, however, go in the opposite direction considering growing security concerns among some EU Member States. A few months after *Schrems II*, the Court in fact recognized EU law did not prohibit mass or targeted surveillance when 'genuine and present or foreseeable' security threats exist and European citizens have access to an independent redress (European Court of Justice 2020, par. 168). The heightened security demands created by the Ukraine war may alter the Court's interpretation of the DPF. If not, the Commission will have gained valuable time before having to look for another solution once more.

Conclusion

Finding a durable solution to regulating privacy remains one of the thorniest issues in the transatlantic digital economy. Over the last two decades, the EU and US signed three successive international agreements supporting the growth of a transatlantic digital economy (Young 2024a this issue). Behind this veneer of cooperation, divergent regulatory approaches yet continuously risk disrupting data flows between the two jurisdictions. This is due to the willingness of both parties to rely on political agreements, driven by economic and geopolitical concerns, even in the face of domestic political opposition. While the Safe Harbor agreement provided a creative political solution, allowing the transatlantic digital economy to flourish despite these differences, the Snowden leaks revealed that privacy protections for EU individuals' data passing through the US were much more limited than assumed. Since then, the Commission has had to navigate the judicial veto point of the ECJ while looking for ways to avoid disruptions to transatlantic data flows.

According to traditional two-level game theory, the negotiation of failed agreements can result from misperceptions surrounding the position of domestic veto points. While the invalidation of Safe Harbor indeed stems from a lack of information regarding the level of protection from US surveillance practices that the agreement afforded and the Court's position, the negotiation of the two following data flow agreements is hard to explain from this perspective. In addition to the Court clarifying its stance in *Schrems I* and *Schrems II*, actors inside and outside of EU institutions sent clear signals, which made repeated miscalculations unlikely.

By tracing the negotiation history of the Privacy Shield and DPF agreements, we argue

that the negotiations reveal an alternative understanding of how international negotiators may act in the face of domestic veto constraints. While attempting to make some changes to alleviate the Court's concerns, the Commission aimed to reap the short-term benefits associated with signing onto agreements that kept the transatlantic digital economy operational, while playing with the uncertainty surrounding the future position of the Court. For the Commission, maintaining transatlantic data flows was imperative both economically and geopolitically, as the need to show unity with the US in international affairs increased. Because it often takes years to activate judicial veto points, an interim agreement can buy valuable time. Moreover, by the time the Court makes a judgement on the DPF, there may be sufficient policy convergence based on changes to privacy legislation in the US or a shift in the preferences of the Court vis-a-vissurveillance practices. As discussed in other articles in this issue (see e.g. Brown 2024; Young 2024a), the evolving geopolitical context may help foster closer cooperation between the transatlantic partners.

At the same time, this strategy of buying time is also a risky one. Every time the ECJ strikes down a data-flow agreement, the Commission risks its legitimacy as the supposed 'guardian of the treaties', mirroring other developments in the intra-EU enforcement of the rule of law (Mandujano Manriquez and Pavone 2024). Thus, while buying time can allow the Commission to realize pressing economic and geopolitical objectives in the short-term, it also carries long-term costs.

Whether this strategy pays off remains to be seen. As of now, the ECJ has yet to change its interpretation of EU privacy law. Its stated preference remains outside of a feasible winset, as seen in Figure 1. The possible change in US privacy laws and signals that the ECJ might change its view surrounding acceptable surveillance practices may lead us closer to the situation portrayed in Figure 2. However, the only certainty for now is that by signing off on the DPF, the Commission has once again temporarily resolved the conflict while issuing for itself a 'round-trip ticket to the ECJ,' as Schrems would say.

More generally, the paper helps scholars to reconsider the politics of the two-level game. Leaders frequently sign onto agreements, which face domestic opposition. Rather than viewing this as irrational or the product of imperfect information, our argument suggests that such behavior is a much more common political strategy – buying for time – in which the temporal uncertainty of veto points opens up additional room for political maneuvering.

Acknowledgments

We are grateful to Alasdair Young for putting together this special issue and to all participants in the 'Governing the Digital Economy' workshop for providing helpful feedback. We also thank two anonymous reviewers and journal editors for their excellent comments on previous drafts of this article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Guillaume Beaumier is an assistant professor in politics and international studies at l'École nationale d'administration publique.

Jonas Heering is a Ph.D. candidate in the Government Department at Georgetown University.

Abraham Newman is a professor in the School of Foreign Service and Government Department at Georgetown University.

ORCID

Guillaume Beaumier: http://orcid.org/0000-0001-9418-6149/ Jonas Heering: http://orcid.org/0009-0008-8426-7867/ Abraham Newman: http://orcid.org/0000-0003-4105-1229

References

Article 29 Working Party. 2016. "Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision." April 13. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

Bach, D., and A. L. Newman. 2007. "The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence." *Journal of European Public Policy* 14 (6): 827–846. https://doi.org/10.1080/13501760701497659.

Beaumier, G. 2023. "Novelty and the Demand for Private Regulation: Evidence from Data Privacy Governance." *Business and Politics* 25 (4): 371–392. https://doi.org/10.1017/bap.2023.16.

Beaumier, G., M. Papin, and J.-F. Morin. 2024. "A Combinatorial Theory of Institutional Invention." *International Theory* 16 (1): 1–27. https://doi.org/10.1017/S1752971923000064.

Bennett, C. 2010. "International Privacy Standards: A Continuing Convergence." *Privacy Laws & Business International Newsletter* 105:13–14. https://dspace.library.uvic.ca/server/api/core/bitstreams/4bc2c556-8a44-413e-b839-b2064ddd4bb1/content.

Bennett, C., and C. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Beutelsbacher, S. 2023. "Europas DATENDEAL mit den USA droht das Nein." *Die Welt*. Accessed February 20, 2023.

Birchfield, V. L. 2024. "From Roadmap to Regulation: Will There Be a Transatlantic Approach to Governing Artificial Intelligence?" *Journal of European Integration* 46 (7).

Bonoli, G. 2001. "Political Institutions, Veto Points, and the Process of Welfare State Adaptation." In *The New Politics of the Welfare State*, edited by Paul Pierson, 238–264. Oxford, UK: Oxford University Press.

Bradford, A. 2012. "The Brussels Effect." *Northwestern University Law Review* 107 (1): 1–68. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1275&context=faculty_scholarship.

Brown, S. A. W. 2024. "Beyond the Great Firewall: EU and US Responses to the China Challenge in the Global Digital Economy." *Journal of European Integration* 46 (7).

Bursens, P., and D. De Bièvre. 2023. "Seizing the Moment: Regional Opportunity Structures and Wallonia's Temporary Veto of the EU–Canada Bilateral Trade Agreement." *Regional & Federal Studies* 33 (1): 113–132. https://doi.org/10.1080/13597566.2021.2007477.

Chander, A., M. E. Kaminski, and W. McGeveran. 2021. "Catalyzing Privacy Law." *Minnesota Law Review* 105 (4): 1732–1802. https://doi.org/10.2139/ssrn.3433922.

Christakis, T., K. Propp, and P. Swire. 2022. "EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers." *European Law Blog* (Blog). February 16, 2022. https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers/.

Damro, C. 2012. "Market Power Europe." *Journal of European Public Policy* 19 (5): 682–699. https://doi.org/10.1080/13501763.2011.646779.

Dewey, M., and D. Di Carlo. 2022. "Governing Through Non - Enforcement: Regulatory Forbearance as Industrial Policy in Advanced Economies." *Regulation & Governance* 16 (3): 930–950. https://doi.org/10.1111/rego.12382.

Drezner, D. W. 2007. *All Politics is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

European Commission. 2013. "Informal Justice Council in Vilnius [Press Release]." July 19. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_710.

European Commission. 2015. "Why We Need a Digital Single Market."December. https://commission.europa.eu/system/files/2015-12/dsm-factsheet_en.pdf.

European Commission. 2016. "European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows [Press Release]."July 12. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461.

European Commission. 2022"Trans-Atlantic Data Privacy Framework." March. https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf.

European Commission. 2023 "Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows [Press Release]."July 10. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

European Court of Justice. 2015 October 6. "The Court of Justice Declares That the Commission's US Safe Harbour Decision is Invalid [Press Release]." https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

European Court of Justice. 2020. October 6. "JUDGMENT of the COURT (Grand Chamber) 6." October 2022. https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=900264.

European Data Protection Board. 2023a. "1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision [Press Release]."May 22. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

European Data Protection Board. 2023b February 28. "Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data Under the EU-US Data Privacy Framework." https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

European Ombudsperson. 2016a. "Follow-Up Reply from the European Ombudsman to Commissioner Jourová on the Use of the Title 'Ombudsperson' in the EU-US Privacy Shield Agreement." https://www.ombudsman.europa.eu/en/doc/correspondence/en/66926.

European Ombudsperson. 2016b February 21. "Use of the Title 'Ombudsman' in the 'EU-US Privacy Shield' Agreement."May 1. https://www.ombudsman.europa.eu/en/doc/correspondence/en/64157.

European Parliament. 2016. "European Parliament Resolution of 26 May 2016 on Transatlantic Data Flows (2016/2727(RSP))."May 26. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0233_EN.pdf?redirect.

European Parliament. 2023. "MEPs Against Greenlighting Personal Data Transfers with the U.S. Under Current Rules [Press Release]."April 13. https://www.europarl.europa.eu/news/en/press-room/20230411IPR79501/meps-against-greenlighting-data-transfers-with-the-u-s-under-current-rules.

Evans, P. B., H. K. Jacobson, and R. D. Putnam. 1993. *Double-Edged Diplomacy: International Bargaining and Domestic Politics*. Berkeley, CA: University of California Press.

Fahey, E. 2024. "The Evolution of EU-US Cybersecurity Law and Policy: On Drivers of Convergence." *Journal of European Integration* 46 (7).

Fahey, E., and F. Terpan. 2023. "The Future of the EU-US Privacy Shield." In *The Routledge Handbook of Transatlantic Relations*, edited by Elaine Fahey, 221–236. Abingdon, UK: Routledge.

Farrell, H. 2003. "Constructing the International Foundations of E-Commerce—the EU-US Safe Harbor Arrangement." *International Organization* 57 (2): 277–306. https://doi.org/10.1017/S0020818303572022.

Farrell, H., and A. L. Newman. 2019. *Of Privacy and Power: The Transatlantic Struggle Over Freedom and Security*. Princeton, NJ: Princeton University Press.

Fefer, R., and K. Archick. 2021. *U.S.-EU Privacy Shield and Transatlantic Data Flows*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46917.

Gunst, S., and F. De Ville. 2021. "The Brussels Effect: How the GDPR Conquered Silicon Valley." *European Foreign Affairs Review* 26 (3): 437–458. https://doi.org/10.54648/EERR2021036.

Hallerberg, M., and S. Basinger. 1998. "Internationalization and Changes in Tax Policy in OECD Countries: The Importance of Domestic Veto Players." *Comparative Political Studies* 31 (3): 321–352. https://doi.org/10.1177/0010414098031003003.

Holland, M. 2023. "U.S. Lawmakers Renew Push on Federal Privacy Legislation." *TechTarget*. Accessed March 3, 2023. https://www.techtarget.com/searchcio/news/365532173/US-lawmakers-renew-push-on-federal-privacy-legislation.

Humphries, C. 2023. "New EU-US Data Pact May Come Too Late for Facebook -Regulator." *Reuters*. Accessed March 7, 2023. https://www.reuters.com/technology/new-eu-us-data-pact-may-come-too-late-facebook-regulator-2023-03-07/.

Kalyanpur, N., and A. Newman. 2019. "The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation." *JCMS: Journal of Common Market Studies* 57 (3): 448–467. https://doi.org/10.1111/jcms.12810.

Keefer, P., and D. Stasavage. 2003. "The Limits of Delegation: Veto Players, Central Bank Independence, and the Credibility of Monetary Policy." *The American Political Science Review* 97 (3): 407–423. https://doi.org/10.1017/S0003055403000777.

Kelemen, R. D. 2010. "Globalizing European Union Environmental Policy." *Journal of European Public Policy* 17 (3): 335–349. https://doi.org/10.1080/13501761003662065.

Kerry, C., and C. Chin-Rothmann. 2020. "How the 2020 Elections Will Shape the Federal Privacy Debate." *Brookings Institution*., October 26. https://www.brookings.edu/articles/how-the-2020-elections-will-shape-the-federal-privacy-debate/.

Kerry, C. F. 2023. "Will the New EU-U.S. Data Privacy Framework Pass CJEU Scrutiny?" *Lawfare*. Accessed August 10, 2023. https://www.lawfaremedia.org/article/will-the-new-eu-u.s.-data-privacy-framework-pass-cjeu-scrutiny.

Laurer, M., and T. Seidl. 2021. "Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation." *Policy & Internet* 13 (2): 257–277. https://doi.org/10.1002/poi3.246.

Li, S., and A. Newman. 2022. "Over the Shoulder Enforcement in European Regulatory Networks: The Role of Arbitrage Mitigation Mechanisms in the General Data Protection Regulation." *Journal of European Public Policy* 29 (10): 1698–1720. https://doi.org/10.1080/13501763.2022.2069845.

Litan, R. E., and P. Swire. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution Press.

Long, W. J., and M. P. Quek. 2002. "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise." *Journal of European Public Policy* 9 (3): 325–344. https://doi.org/10.1080/13501760210138778.

MacMillan, R. 2000, July 27. "EC Adopts Data Privacy Plan Despite Concerns." *Newsbytes*. (Retriev via Factiva).

Manancourt, V. 2022. "EU Justice Chief Confident New US Data Pact Will Survive Legal Challenge." *Politico*. Accessed December 12, 2022. https://www.politico.eu/article/eu-justice-chief-confident-new-us-data-pact-will-survive-legal-challenge/.

Manancourt, V., and M. Scott. 2021. "Washington Says a Transatlantic Data Deal is Close. Brussels Disagrees." *Politico*. Accessed September 17, 2021. https://www.politico.eu/article/washington-transatlantic-data-deal-brussels/.

Mandujano Manriquez, M., and T. Pavone. 2024. "Follow the Leader: The European Commission, the European Court of Justice, and the EU's Rule of Law Revolution." *Working Paper*. https://preprints.apsanet.org/engage/apsa/article-details/65d623cf9138d23161a6f674.

Manners, I. 2002. "Normative Power Europe: A Contradiction in Terms?" *JCMS: Journal of Common Market Studies* 40 (2): 235–258. https://doi.org/10.1111/1468-5965.00353.

Mansfield, E. D., H. V. Milner, and J. C. Pevehouse. 2007. "Vetoing Co-Operation: The Impact of Veto Players on Preferential Trading Arrangements." *British Journal of Political Science* 37 (3): 403–432. https://doi.org/10.1017/S0007123407000221.

Mazur, J., and M. Serafin. 2023. "Stalling the State: How Digital Platforms Contribute to and Profit from Delays in the Enforcement and Adoption of Regulations." *Comparative Political Studies* 56 (1): 101–130. https://doi.org/10.1177/00104140221089651.

Meltzer, J. P. 2016, October. "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment." Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf.

Milner, H. V., and B. P. Rosendorff. 1997. "Democratic Politics and International Trade Negotiations: Elections and Divided Government as Constraints on Trade Liberalization." *The Journal of Conflict Resolution* 41 (1): 117–146. https://doi.org/10.1177/0022002797041001006.

Newman, A. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca, NY: Cornell University Press.

Noyb. 2022, May. "Open Letter Announcement of a New EU-US Personal Data Transfer Framework." https://noyb.eu/sites/default/files/2022-05/open_letter_EU-US_agreement.pdf.

Noyb. 2023, July 10. "European Commission Give EU-US Data Transfers Third Round at CJEU." https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Obinger, H., S. Leibfried, and F. G. Castles. 2005. "Bypasses to a Social Europe? Lessons from Federal Experience." *Journal of European Public Policy* 12 (3): 545–571.

O'Donnell, J. 2013. "EU Demands Protection Against U.S. Data Surveillance." Reuters. Accessed November 26, 2013. https://www.reuters.com/article/us-eu-data/eu-demands-protection-against-u-s-data-surveillance-idUSBRE9AP0NW20131126.

O'reilly, R. F. 2005. "Veto Points, Veto Players, and International Trade Policy." *Comparative Political Studies* 38 (6): 652–675. https://doi.org/10.1177/0010414004274379.

Propp, K. 2023. "Revenge, or Reciprocity? The U.S.'s Review of Europe's SIGINT Safeguards." *Lawfare*. Accessed August 29, 2023. https://www.lawfaremedia.org/article/revenge-or-reciprocity-the-u.s.-s-review-of-europe-s-sigint-safeguards.

Putnam, R. D. 1988. "Diplomacy and Domestic Politics: The Logic of Two-Level Games." *International Organization* 42 (3): 427–460. https://doi.org/10.1017/S0020818300027697.

Schrems, M. 2016. "'EU US Privacy Shield' (Safe Harbor 1.1) – 'European Commission May Be Issuing a Round-Trip to Luxembourg'." http://europe-v-facebook.org/PS_update.pdf. Europe versus Facebook.

Schwartz, P. M., and K.-N. Pfeifer. 2017. "Transatlantic Data Privacy Law." *The Georgetown Law Journal* 106 (1): 115–179. https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-106/volume-106-issue-1-november-2017/transatlantic-data-privacy-law/.

Scott, M. 2021. "US Offers Deal to Woo Europe on Data." *Politico*. Accessed October 21, 2021. https://www.politico.eu/article/negotiations-for-new-transatlantic-data-deal-nudge-forward/.

Scott, M., and V. Manancourt. 2021. "Europe to US: Pass New Laws if You Want a Data-Transfer Deal." *Politico*. Accessed June 1, 2021. https://www.politico.eu/article/europe-to-us-pass-new-laws-if-you-want-data-transfer-deal-privacy-regulation/.

Scott, M., and V. Manancourt. 2022. "US Eyes Breakthrough on Data Dispute with EU as Biden Visits Brussels." *Politico*. Accessed March 24, 2022. https://www.politico.eu/article/us-eyes-breakthrough-on-data-dispute-with-eu-biden-visit-privacy-shield-ukraine/.

Shahin, J. 2024. "Dancing to the Same Tune? EU and US Approaches to Standards Setting in the Global Digital Sector." *Journal of European Integration* 46 (7).

Stupp, C. 2017. "EU Privacy Watchdog: Privacy Shield Should Be Temporary." *Euractiv*. August 3. https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/.

Stupp, C. 2023. "Ukraine War Shows Need for Global Data-Privacy Agreement, EU Officials Say." *The Wall Street Journal*. Accessed March 25, 2023. https://www.wsj.com/articles/ukraine-war-shows-

need-for-global-data-privacy-agreement-eu-officials-say-11653471001.

Swire, P. 2020. "'Schrems II' Backs the European Legal Regime into a Corner — How Can it Get Out?" IAPP. Accessed March 25, 2023. July 16. https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/.

Terpan, F., and S. Saurugger. 2019. "Assessing Judicial Activism of the CJEU the Case of the court's Defence Procurement Rulings." *Journal of European Integration* 41 (4): 543–561. https://doi.org/10.1080/07036337.2018.1537268.

Tsebelis, G. 1999. "Veto Players and Law Production in Parliamentary Democracies: An Empirical Analysis." *The American Political Science Review* 93 (3): 591–608. https://doi.org/10.2307/2585576.

Tsebelis, G. 2000. "Veto Players and Institutional Analysis." *Governance-An International Journal of Policy Administration and Institutions* 13 (4): 441–474. https://doi.org/10.1111/0952-1895.00141.

Tsebelis, G. 2002. *Veto Players: How Political Institutions Work*. Princeton, NJ: Princeton University Press.

US Department of Commerce. 2012. "U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson [Press Release]." March 19. https://2010-2014.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re.html.

Voeten, E. 2008. "The Impartiality of International Judges: Evidence from the European Court of Human Rights." *The American Political Science Review* 102 (4): 417–433. https://doi.org/10.1017/S0003055408080398.

Von Der Leyen, U. 2022. "The Transatlantic Partnership Stands Stronger Than Ever. In a World Faced with Disorder, Our Unity Upholds Fundamental Values and Rules That Our Citizens Believe In. And We are Determined." Accessed March 25, 2022. https://twitter.com/vonderleyen/status/1507282881772765201.

The White House. 2022. "FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework."March 25. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

Young, A. R. 2024a. "Governing the Digital Economy: Transatlantic Accommodation and Cooperation." *Journal of European Integration* 46 (7).

Young, A. R. 2024b. "Triumph in Taxing Times? Linked Transatlantic Two-Level Games and the Taxation of the Digital Economy." *Journal of European Integration* 46 (7).